

Asymptotically optimal approximation of single qubit unitaries by Clifford and T circuits using a constant number of ancillary qubits

Vadym Kliuchnikov¹, Dmitri Maslov^{2,3}, and Michele Mosca^{4,5}

¹ *Institute for Quantum Computing, and David R. Cheriton School of Computer Science*

University of Waterloo, Waterloo, Ontario, Canada

² *National Science Foundation*

Arlington, Virginia, USA

³ *Institute for Quantum Computing, and Dept. of Physics & Astronomy*

University of Waterloo, Waterloo, Ontario, Canada

⁴ *Institute for Quantum Computing, and Dept. of Combinatorics & Optimization*

University of Waterloo, Waterloo, Ontario, Canada

⁵ *Perimeter Institute for Theoretical Physics*

Waterloo, Ontario, Canada

December 7, 2012

Abstract

We present an algorithm for building a circuit that approximates single qubit unitaries with precision ε using $O(\log(1/\varepsilon))$ Clifford and T gates and employing up to two ancillary qubits. The algorithm for computing our approximating circuit requires an average of $O(\log^2(1/\varepsilon) \log \log(1/\varepsilon))$ operations. We prove that the number of gates in our circuit saturates the lower bound on the number of gates required in the scenario when a constant number of ancillae are supplied, and as such, our circuits are asymptotically optimal. This results in significant improvement over the current state of the art for finding an approximation of a unitary, including the Solovay-Kitaev algorithm that requires $O(\log^{3+\delta}(1/\varepsilon))$ gates and does not use ancillae and the phase kickback approach that requires $O(\log^2(1/\varepsilon) \log \log(1/\varepsilon))$ gates, but uses $O(\log^2(1/\varepsilon))$ ancillae.

1 Introduction

The efficient approximation of a unitary using a discrete universal gate set is crucial for building a scalable quantum computing device. Barenco *et al.* [1] showed that any unitary may be implemented by a circuit with CNOT and single qubit gates, effectively reducing the problem to that of the single qubit unitary synthesis/approximation. A constructive answer to the question of how to approximate a single qubit unitary by a quantum circuit is given by the Solovay-Kitaev algorithm [2, 3]. While the Solovay-Kitaev algorithm may be applied to approximating multiple qubit/qudit unitaries by quantum circuits, in practice it remains most useful for single qubit approximations.

Technically, the problem of single qubit circuit synthesis is formulated as follows: given a discrete universal gate set or “library”, find a sequence of gates in it that approximates a given unitary with precision ε . Parameter ε determines complexity of the resulting approximation.

Computing an approximation using the standard version of the Solovay-Kitaev algorithm [3] takes $O(\log^{2.71}(1/\varepsilon))$ steps on a classical computer and the number of gates in the resulting quantum circuit is $O(\log^{3.97}(1/\varepsilon))$. The best known upper bound on the circuit size resulting from the application of the Solovay-Kitaev algorithm is $O(\log^{3+\delta}(1/\varepsilon))$, where δ can be chosen arbitrary small [2]. From the other side, Harrow *et al.* [4] show an $\Omega(\log(1/\varepsilon))$ lower bound on the number of gates in the approximating circuit. A certain library of quantum gates that allows approximating a single qubit unitary to precision ε with a circuit containing at most $O(\log(1/\varepsilon))$ gates is also reported in [4]. However, no efficient algorithm to construct a circuit meeting the lower bound in the number of gates is known. Furthermore, the gate set used, $\frac{I+2i\{X,Y,Z\}}{\sqrt{5}}$, is not considered to be well-suited for a fault-tolerant implementation, in contrast to the Clifford and T library. To the best of our knowledge, constructive saturation of the logarithmic lower bound in the Clifford and T library has not been shown yet, however, numerical evidence supports the theory that this is indeed the case [5] (based on an exponential-time breadth first search algorithm). Our result comes close to exactly meeting the

lower bound—our gate count is logarithmic, $O(\log(1/\varepsilon))$, however, we use an additional resource in the form of at most two qubits initialized to the state $|0\rangle$.

Allowing additional resources helps to achieve interesting improvements over the Solovay-Kitaev algorithm. For example, using a special resource state $|\gamma\rangle$ on $O(\log(1/\varepsilon))$ qubits allows to achieve the desired accuracy of approximation by a depth $O(\log(\log(1/\varepsilon)))$ circuit containing $O(\log(1/\varepsilon))$ gates [2], also known as phase kickback algorithm. However, the resource state preparation requires $O(\log^2(1/\varepsilon))$ ancillae qubits and a circuit of depth $O(\log^2(\log(1/\varepsilon)))$ containing $O(\log^2(1/\varepsilon) \log \log(1/\varepsilon))$ gates. Furthermore, exact preparation of the resource state $|\gamma\rangle$ is not possible using gates from the Clifford and T library and qubits initialized to $|0\rangle$ [7, 8]. In comparison, in our work, we employ only two ancillae prepared in the simple state $|0\rangle$, and this results in achieving the approximating accuracy of ε using a circuit with $O(\log(1/\varepsilon))$ gates. Later in the paper we show the lower bound of $\Omega(\log(1/\varepsilon))$ on the number of gates required to approximate a unitary to the accuracy ε using a fixed number of ancillae initialized to $|0\rangle$ and any universal gate set. One other recent approach uses resource states [6] and probabilistic circuits with classical feedback. The circuit itself, excluding state preparation, requires on average a constant number of operations and a constant number of ancilla qubits. The method requires precomputed ancillae in the states $R_Z(2^n \phi)H|0\rangle$ to implement $R_Z(2^m \phi)$. Our algorithm does not rely on the measurements and classical feedback, and our circuit is deterministic. More importantly, our algorithm does not employ sophisticated ancilla states that, in turn, may require approximation, as they may not be possible to prepare exactly in the Clifford and T library [7, 8].

In our previous work [7], we showed that any single qubit unitary with entries u_{ij} in the ring $\mathbb{Z}\left[i, \frac{1}{\sqrt{2}}\right]$ can be synthesized exactly using single qubit Clifford and T gates. Furthermore, we presented an asymptotically optimal algorithm for finding a circuit with the minimal number of Hadamard gates and asymptotically minimal total number of gates. More precisely, if the square of the norm of an element of the single qubit unitary matrix, $|u_{ij}|^2$, can be represented as $(a + \sqrt{2}b)/2^n$, where a and b are integers such that $GCD(a, b)$ is odd, the total number of gates required to synthesize the unitary is in $\Theta(n)$. This work opened the door for bypassing the Solovay-Kitaev algorithm for fast circuit approximation of single qubit unitaries by efficiently approximating arbitrary unitaries with unitaries over the ring $\mathbb{Z}\left[i, \frac{1}{\sqrt{2}}\right]$. However, to date, no efficient ring round-off procedure was reported, and it remains an important open problem.

Giles and Selinger [8] recently found an elegant way to prove the conjecture formulated in [7] stating that multiple qubit unitaries over the ring $\mathbb{Z}\left[i, \frac{1}{\sqrt{2}}\right]$ may be synthesized exactly using Clifford and T library. In this paper, we employ some of their results to show that, by adding at most two ancilla qubits, we can achieve asymptotically optimal approximation of the single qubit unitaries in the Clifford and T library.

The significance of the improvement provided by our approach is best seen when, for a fixed precision ε , all of the approximating circuit parameters such as depth, the number of gates, and ancillae are added into one aggregate figure, such as, e.g., the product of the three of these parameters.

2 Main result

We focus on the approximation of the following operator:

$$\Lambda(e^{i\phi}) : \alpha|0\rangle + \beta|1\rangle \mapsto \alpha|0\rangle + \beta e^{i\phi}|1\rangle.$$

We note that any single qubit unitary can be decomposed in terms of a constant number of Hadamard gates and $\Lambda(e^{i\phi})$ (see solution to Problem 8.1 in [2]). Therefore, the ability to approximate $\Lambda(e^{i\phi})$ implies the ability to approximate any single qubit unitary.

There are two main steps in our algorithm:

1. Find a circuit C consisting of Clifford and T gates such that the result of applying C to $|00\rangle$ is close to $e^{i\phi}|00\rangle$.
2. Apply circuit C controlled on the first qubit to perform a transformation close to:

$$\alpha|000\rangle + \beta|100\rangle \mapsto \alpha|000\rangle + \beta e^{i\phi}|100\rangle.$$

It can be observed that the net effect of such transformation may be described as the application of $\Lambda(e^{i\phi})$ to the first qubit. To accomplish the first step we approximate $e^{i\phi}|00\rangle$ with a four dimensional vector $|v\rangle$ with entries in the ring $\mathbb{Z}\left[i, \frac{1}{\sqrt{2}}\right]$. We then employ an algorithm for multiple qubit exact synthesis to find a circuit C that prepares $|v\rangle$ starting from $|00\rangle$ using at most one ancilla qubit. It was shown in [9] that any circuit using Clifford and T gates can be transformed into its exact (meaning no further approximation is required) controlled version with only a linear

overhead in the number of gates, and using at most one ancilla qubit in the state $|0\rangle$ that is returned unchanged. Our analysis shows that, however, on this step we do not need to use this additional ancilla. The resulting total number of ancillae is thus at most two.

2.1 Approximating $e^{i\phi} |00\rangle$

The key is the reduction of the approximation problem to expressing an integer number as a sum of four squares. In particular, we are looking for an approximation of:

$$e^{i\phi} |00\rangle = (\cos(\phi) + i \sin(\phi), 0, 0, 0)$$

by a unit vector:

$$|v\rangle := \frac{1}{2^k} (\lfloor 2^k \cos(\phi) \rfloor + i \lfloor 2^k \sin(\phi) \rfloor, 0, a + ib, c + id),$$

where $k \in \mathbb{N}; a, b, c, d \in \mathbb{Z}$. Without loss of generality we can assume that $0 \leq \phi \leq \frac{\pi}{4}$. The power k of the denominator determines precision of our approximation and complexity of the resulting circuit. As $|v\rangle$ must be a unit vector, the remaining four parameters (a, b, c , and d) should satisfy the integer equation:

$$a^2 + b^2 + c^2 + d^2 = 4^k - \lfloor 2^k \cos(\phi) \rfloor^2 - \lfloor 2^k \sin(\phi) \rfloor^2.$$

Lagrange's four square theorem states that this equation always has a solution. Furthermore, there exists an efficient probabilistic algorithm for finding a solution. For the right hand side M it requires on average $O(\log^2(M) \log \log M)$ operations with integers smaller than M . It is described in Theorem 2.2 in [10]. We get a reduction to such a simple Diophantine equation at the expense of using two qubits instead of one.

Furthermore, in estimating the classical complexity of the algorithm for finding the approximating circuit, we will rely on an observation that

$$4^k - \lfloor 2^k \cos(\phi) \rfloor^2 - \lfloor 2^k \sin(\phi) \rfloor^2 \leq 4 \times 2^k + \text{Const} \in O(2^k).$$

2.2 Precision and complexity analysis

Let us introduce $\gamma = (\lfloor 2^k \cos(\phi) \rfloor + i \lfloor 2^k \sin(\phi) \rfloor) / 2^k$ and express $|v\rangle$ as:

$$|v\rangle = \gamma |00\rangle + |1\rangle \otimes |g\rangle.$$

The application of the circuit C controlled on the first qubit will transform $(\alpha |0\rangle + \beta |1\rangle) \otimes |00\rangle$ into:

$$\alpha |000\rangle + \beta \gamma |100\rangle + \beta |01\rangle \otimes |g\rangle.$$

The distance of the result to the desired state $\alpha |000\rangle + \beta e^{i\phi} |100\rangle$ is:

$$\sqrt{|\beta(e^{i\phi} - \gamma)|^2 + |\beta|^2 \| |g\rangle \|^2}.$$

By the choice of γ we have $|\gamma - e^{i\phi}| \leq \frac{\sqrt{2}}{2^k}$, therefore the first term in the sum above is in $O(1/2^{2k})$. The norm squared of $|g\rangle$ equals $1 - |\gamma|^2$. The complex number γ approximates $e^{i\phi}$, and the distance of its absolute value to identity can be estimated using the triangle inequality:

$$||\gamma| - |e^{i\phi}|| \leq |\gamma - e^{i\phi}|.$$

Therefore, $1 - |\gamma|^2$ is in $O(1/2^k)$. In summary, the distance to the approximation is in $O(1/2^{0.5k})$.

The same estimate is true if we consider the circuit C as a part of a larger system. In this case we should start with the state $(\alpha |\phi_0\rangle \otimes |0\rangle + \beta |\phi_1\rangle \otimes |1\rangle) \otimes |00\rangle$. Similar analysis shows that the distance to approximation remains $O(1/2^{0.5k})$.

As shown in [8], it is possible to find a circuit that prepares $|v\rangle$ using $O(k)$ Clifford and T gates ([8], Lemma 20 (Column lemma)). The classical complexity of constructing a quantum circuit implementing $|v\rangle$ is in $O(k)$. In the controlled version of this circuit the number of gates remains $O(k)$ ([9], Theorem 1). In summary, we need $O(\log(1/\varepsilon))$ gates to achieve precision ε . The complexity of the classical algorithm for constructing the entire approximating circuit is thus dominated by complexity of finding a solution to the Diophantine equation, which is in $O(\log^2(1/\varepsilon) \log \log(1/\varepsilon))$.

2.3 How many ancillae are needed?

A straightforward calculation shows that the number of ancillae used is three. However, we can get around using only two ancillae. To understand how, we need to go into the details of the proof of Lemma 20 (Column lemma) from [8]. It shows how to find a sequence of two-level unitaries of type iX , $T^{-m}(iH)T^m$, and W [8] and length $O(k)$ that allows to prepare a state with the denominator 2^k . A controlled version of the two level unitary is again a two level unitary. In [8], Lemma 24, it was also shown that any such unitary required can be implemented using no extra ancillae. Therefore, the controlled version of the circuit C will not use any additional ancilla and we need only two of them in total.

3 Lower bound on the number of gates when ancillae are allowed

Lemma 1. *Let G be a universal library, and let M_V be a set of unitaries, that simulate a unitary V acting on n qubits, using m ancillary qubits:*

$$M_V = \{U \in \mathbb{U}(2^{m+n}) \mid U(|0\rangle \otimes |\phi\rangle) = |0\rangle \otimes (V|\phi\rangle)\}.$$

Then, for any ε there always exists a unitary $V(\varepsilon)$ such that the number of gates from G needed to construct a unitary within the distance ε to $M_{V(\varepsilon)}$ is in $\Omega(\log(1/\varepsilon))$.

We use the volume argument similar to the one presented in [4].

Let $N = 2^n$, ρ be the distance induced by Frobenius norm and μ be the Haar measure on $\mathbb{U}(N)$. For the unitary U we define the volume of its ε -neighbourhood as:

$$v(U, \varepsilon) = \mu\{V \in \mathbb{U}(N) \mid \rho(M_V, U) \leq \varepsilon\}.$$

Let G^k be the set of all unitaries that can be constructed using k gates from the library G . Suppose that for any unitary V we can find a unitary U from G^k within the distance ε from M_V . This implies:

$$\mu(\mathbb{U}(N)) \leq \sum_{U \in G^k} v(U, \varepsilon) \leq |G|^k \max_{U \in G^k} v(U, \varepsilon).$$

We will show that the volume $v(U, \varepsilon)$ is upper bounded by $C_0 \varepsilon^{N^2}$, for some constant C_0 , therefore:

$$k \geq \frac{1}{\log |G|} \log \left(\frac{\mu(\mathbb{U}(N))}{C_0 \varepsilon^{N^2}} \right). \quad (1)$$

We next show how to estimate $v(U, \varepsilon)$. Let U_0 be a submatrix of U defined as follows:

$$U_0 := \{\langle e_i | \otimes \langle 0 | \rangle U | 0 \rangle \otimes | e_j \rangle\}$$

where $\{|e_i\rangle\}$ is the standard (computational) basis in $\mathbb{C}(N)$. Taking into account that the distance ρ is induced by Frobenius norm, we write $\rho(U, M_V) \geq \rho(U_0, V)$. Therefore:

$$v(U, \varepsilon) = \mu\{V \mid \rho(M_V, U) < \varepsilon\} \leq \mu\{V \mid \rho(U_0, V) < \varepsilon\}.$$

Let us define V_{min} to be a unitary closest to U_0 . To estimate $v(U, \varepsilon)$ it suffices to consider the case when $\rho(V_{min}, U_0) < \varepsilon$.

The distance ρ is unitarily invariant, therefore $\rho(V_{min}^\dagger U_0, I) < \varepsilon$ and

$$\{V \mid \rho(U_0, V) < \varepsilon\} = \{V \mid \rho(V_{min}^\dagger U_0, V) < \varepsilon\}.$$

From the triangle inequality,

$$\rho(I, V) \leq \rho(V_{min}^\dagger U_0, I) + \rho(V_{min}^\dagger U_0, V),$$

we conclude that

$$\{V \mid \rho(V_{min}^\dagger U_0, V) < \varepsilon\} \subseteq \{V \mid \rho(I, V) < 2\varepsilon\}.$$

Finally,

$$v(U, \varepsilon) \leq \mu\{V \mid \rho(I, V) < 2\varepsilon\}.$$

As shown in [4], there exists a constant C_0 such that the volume of the ball $\{V \mid \rho(I, V) < 2\varepsilon\}$ is less than $C_0 \varepsilon^{N^2}$.

Estimate (1) on k shows that we need circuits of the size at least $\Omega(\log(1/\varepsilon))$ to cover the full group $\mathbb{U}(N)$. If k is chosen in such a way that the inequality (1) does not hold, due to the volume argument, there exists a unitary $V(\varepsilon)$ such that it is not possible to approximate any unitary from $M_{V(\varepsilon)}$ with precision ε using at most k gates.

4 Future work

There are some interesting questions that remain to be answered. The first one concerns the practicality of the proposed construction. In particular, what are the constants hidden behind the big- O notation in our approach, and can they be optimized (while further optimizations are only possible up to a multiplicative factor they are, nevertheless, important for practical purposes)? The original algorithm proposed in [8] uses a decomposition into single and two level unitaries. Each single and two level unitary may have a relatively large (yet, resulting in a blow up by at most a constant factor, [9]) implementation cost. An example is given by the CNOT gate, whose controlled version, the Toffoli gate, requires a strictly positive number of T gates, whereas none are needed for constructing the CNOT itself. Furthermore, T gate is known to be more difficult to implement fault tolerantly compared to any of the Clifford gates. Next, what are the possible trade-offs between adding/reducing ancillae and the gate count? Is it possible to use other efficiently solvable Diophantine equations to discover approximations of other types of gates? Lastly, does there exist an efficient algorithm to round off single-qubit unitaries to those single-qubit unitaries over the ring $\mathbb{Z}\left[i, \frac{1}{\sqrt{2}}\right]$ and avoid the need for ancillary qubits altogether?

5 Acknowledgments

Authors supported in part by the Intelligence Advanced Research Projects Activity (IARPA) via Department of Interior National Business Center Contract number DIIPC20166. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of IARPA, DoI/NBC or the U.S. Government.

Michele Mosca is also supported by Canada's NSERC, MPrime, CIFAR, and CFI. IQC and Perimeter Institute are supported in part by the Government of Canada and the Province of Ontario.

We wish to thank Alex Bocharov, Martin Roetteler, and Peter Selinger for their comments and helpful discussions.

References

- [1] A. Barenco, C. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Physical Review A*, vol. 52, no. 5, pp. 3457–3467, November 1995. <http://arxiv.org/abs/quant-ph/9503016>
- [2] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and Quantum Computation*, ser. Graduate studies in mathematics, v. 47. Boston, MA, USA: American Mathematical Society, 2002.
- [3] C. M. Dawson and M. A. Nielsen, "The Solovay-Kitaev algorithm," *Quantum Information & Computation*, vol. 6, no. 1, pp. 81–95, May 2005. <http://arxiv.org/abs/quant-ph/0505030>
- [4] A. W. Harrow, B. Recht, and I. L. Chuang, "Efficient discrete approximations of quantum gates," *Journal of Mathematical Physics*, vol. 43, no. 9, pp. 4445–4451, November 2002. <http://arxiv.org/abs/quant-ph/0111031>
- [5] A. G. Fowler, "Constructing arbitrary Steane code single logical qubit fault-tolerant gates," *Quantum Information & Computation*, vol. 11, no. 9, p. 8, November 2011. <http://arxiv.org/abs/quant-ph/0411206>
- [6] N. C. Jones, J. D. Whitfield, P. L. McMahon, M.-h. Yung, R. Van Meter, A. Aspuru-Guzik, and Y. Yamamoto, "Simulating chemistry efficiently on fault-tolerant quantum computers," April 2012. <http://arxiv.org/abs/1204.0567>
- [7] V. Kliuchnikov, D. Maslov, and M. Mosca, "Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates," June 2012. <http://arxiv.org/abs/1206.5236>
- [8] B. Giles and P. Selinger, "Exact synthesis of multi-qubit Clifford+T circuits," December 2012. <http://arxiv.org/abs/1212.0506>
- [9] M. Amy, D. Maslov, M. Mosca, and M. Roetteler, "A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits," June 2012. <http://arxiv.org/abs/1206.0758>
- [10] M. O. Rabin and J. O. Shallit, "Randomized algorithms in number theory," *Communications on Pure and Applied Mathematics*, vol. 39, no. S1, pp. S239–S256, 1986.